

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-276443

(43)Date of publication of application : 06.10.2000

(51)Int.Cl.

G06F 15/00

G06F 12/00

G06F 17/30

(21)Application number : 11-079252

(71)Applicant : FUJI XEROX CO LTD

(22)Date of filing : 24.03.1999

(72)Inventor : KAMEOKA MASATO

KURABE ATSUSHI

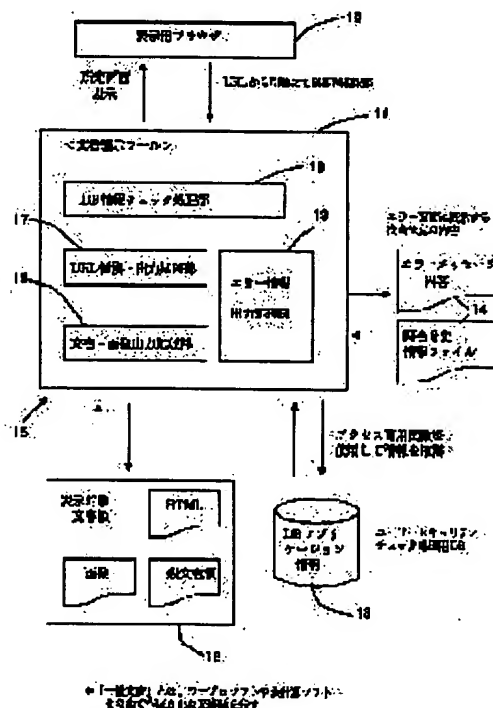
HORI KIWAMU

(54) DOCUMENT DISPLAY DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To easily secure the security of each document even in environments where documents are distributed by link information.

SOLUTION: Link information of an HTML document displayed on a browser 10 for display is an URL passing a check URL substitution program; and when link information is designated to request a page, a data base information check processing part 16 performs authentication or the like of user's authority for access, and the page is sent to the browser 10 only when authentication or the like is successful. If the target file is an HTML file, a URL substitution and output processing part 17 converts the URL included there to a URL passing the check URL substitution program before it is sent to the browser.



LEGAL STATUS

[Date of request for examination]

30.07.2003

[Date of sending the examiner's decision of

rejection]

[Kind of final disposal of application other than
the examiner's decision of rejection or
application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's
decision of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2000-276443
(P2000-276443A)

(43) 公開日 平成12年10月6日 (2000.10.6)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 A 5 B 0 7 5
12/00	5 3 7	12/00	5 3 7 A 5 B 0 8 2
	5 4 6		5 4 6 B 5 B 0 8 5
17/30		15/40	3 1 0 F
			3 2 0 B

審査請求 未請求 請求項の数 9 O L (全 11 頁) 最終頁に続く

(21) 出願番号	特願平11-79252	(71) 出願人	000005496 富士ゼロックス株式会社 東京都港区赤坂二丁目17番22号
(22) 出願日	平成11年3月24日 (1999.3.24)	(72) 発明者	亀岡 正人 神奈川県海老名市本郷2274番地 富士ゼロックス株式会社海老名事業所内
		(72) 発明者	倉部 淳 神奈川県海老名市本郷2274番地 富士ゼロックス株式会社海老名事業所内
		(74) 代理人	100086531 弁理士 澤田 俊夫

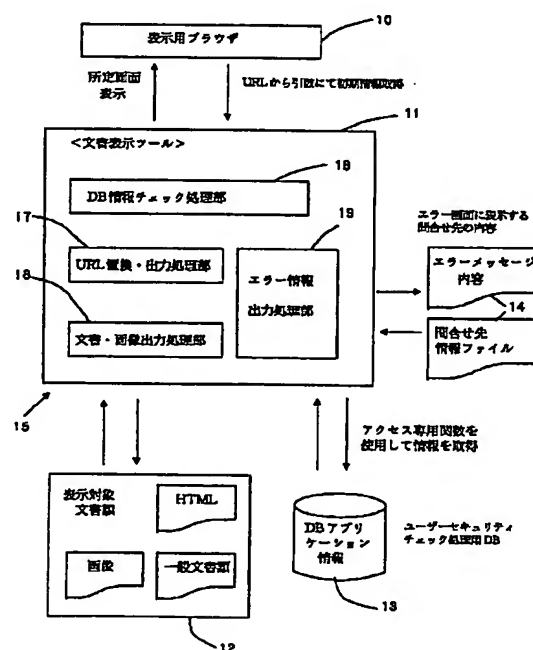
最終頁に続く

(54) 【発明の名称】 文書表示装置

(57) 【要約】

【課題】 リンク情報により文書が分散される環境においても簡易に各文書のセキュリティを確保する。

【解決手段】 表示用ブラウザ10は表示されているHTML文書のリンク情報は、チェック・URL置換プログラム経由のURLとなっており、リンク情報を指定してページをリクエストすると、データベース情報チェック処理部16がユーザのアクセス権限の認証等を行い、認証等が成功したときのみページをブラウザ10に送る。さらにターゲットのファイルがHTMLファイルの場合は、ブラウザに送る前に、URL置換・出力処理部17が、そこに含まれるURLをチェック・URL置換プログラム経由のURLに変換する。



*「一般文書」とは、ワープロソフトや表計算ソフト
その他で作成された文書類を指す

【特許請求の範囲】

【請求項 1】 ブラウザと、

文書ファイルへのアドレス情報を引数として受け取って上記文書ファイルに関するユーザのアクセス権限を認証する認証用プログラム部と、

認証対象の文書ファイルのアドレス情報を上記認証用プログラム部に引数として渡すことを指示するリンク情報を保持するハイパーテキスト文書を記憶する文書記憶手段と、

上記ブラウザに表示されている上記ハイパーテキスト文書中の上記リンク情報を利用して上記認証用プログラム部に上記認証対象の文書ファイルのアドレス情報を引数として送る手段と、

上記認証対象の文書ファイルについて上記認証用プログラム部による認証が成功したときに、上記認証対象のファイルを上記ブラウザに供給する手段とを有することを特徴とする文書表示装置。

【請求項 2】 ブラウザと、

文書ファイルへのアドレス情報を引数として受け取って上記文書ファイルに関するユーザのアクセス権限を認証する認証用プログラム部と、

認証対象の文書ファイルのアドレス情報を上記認証用プログラム部に引数として渡すことを指示するリンク情報を保持するハイパーテキスト文書を記憶する文書記憶手段と、

上記ブラウザに表示されている上記ハイパーテキスト文書中の上記リンク情報を利用して上記認証用プログラム部に上記認証対象の文書ファイルのアドレス情報を引数として送る手段と、

上記認証対象の文書ファイルについて上記認証用プログラム部による認証が成功したときに、上記認証対象のファイルを上記ブラウザに供給する手段と、

上記認証対象の文書ファイルがハイパーテキスト文書の場合には、上記文書ファイルを上記ブラウザに送る前に、上記文書ファイルに含まれる他の文書ファイルへのリンク情報を、上記他の文書ファイルのアドレス情報を上記認証用プログラム部に引数として渡すことを指示するリンク情報に書き換える手段とを有することを特徴とする文書表示装置。

【請求項 3】 上記ハイパーテキスト文書中の他の文書のアドレスは相対パスで記述される請求項 2 記載の文書表示装置。

【請求項 4】 上記認証用プログラムはユーザがアクセスしようとしている文書が提供されるアプリケーションに関する情報を利用して上記ユーザのアクセス権限を認証する請求項 1、2 または 3 記載の文書表示装置。

【請求項 5】 上記認証用プログラム部による認証が失敗したときに上記ブラウザにエラーメッセージのコンテンツを供給するようにした文書表示装置。

【請求項 6】 ハイパーテキスト文書を利用したアプリ

ケーション・サービスにおいてユーザのアクセス権限を認証するアクセス権限認証装置において、

文書ファイルへのアドレス情報を引数として受け取って上記文書ファイルに関するユーザのアクセス権限を認証する認証用プログラム部と、

ブラウザに表示されている上記ハイパーテキスト文書中のリンク情報を利用して上記認証用プログラム部に上記認証対象の文書ファイルのアドレス情報を引数として送る手段とを有することを特徴とするアクセス権限認証装置。

【請求項 7】 リクエストに含まれる URL により、認証を行うプログラムを指定するとともに、上記プログラムの引数として認証対象のファイルのアドレス情報を指定し、上記認証を行うプログラムにより上記認証対象のファイルについてユーザのアクセス権限を認証することを特徴とするアクセス権限認証装置。

【請求項 8】 文書を記憶し認証用プログラム部の認証が成功したときに文書を供給する文書サーバにおいて、認証対象の文書ファイルのアドレス情報を上記認証用プログラム部に引数として渡すことを指示するリンク情報を保持するハイパーテキスト文書を記憶する文書記憶手段を有することを特徴とする文書サーバ。

【請求項 9】 文書についてのユーザのアクセス権限を認証する認証用プログラム部とともに利用されるハイパーテキスト文書変換装置において、

ハイパーテキスト文書に含まれる他の文書ファイルへのリンク情報を、上記他の文書ファイルのアドレス情報を上記認証用プログラム部に引数として渡すことを指示するリンク情報に書き換えることを特徴とするハイパーテキスト文書変換装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、ユーザのアクセス権限を認証し、認証が成功したときに文書をユーザに表示する文書表示装置に関する。

【0002】

【従来の技術】 近年、事業所内においてインターネットの基盤技術を利用して情報処理システムを構築するようになってきている。このようないわゆるイントラネット環境の下では、とくに、HTML（ハイパーテキストマークアップラングエッジ）のウェブサーバとブラウザ（クライアント）とを用いて利用者間で情報やサービスを容易に共有できるようになってきている。

【0003】 またイントラネット環境においても他の情報処理環境と同様に、事業所内の情報やサービスに種々の権限レベルがあり、ユーザのアクセス権限に応じて利用を許可したり、禁止したりする必要がある。

【0004】 ところで、HTML 文書等のハイパーテキストの文書では、アンカータグ等のリンク情報を用いて分散的に文書が配置され、各文書ごとにセキュリティを

確保する手段を構築するのは煩雑となる。

【0005】

【発明が解決する課題】この発明は、以上の事情を考慮してなされたものであり、リンク情報により文書が分散される環境においても簡易に各文書のセキュリティを確保できる文書表示装置を提供することを目的としている。

【0006】

【課題を解決するための手段】この発明によれば、上述の目的を達成するために、文書表示装置に、ブラウザと、文書ファイルへのアドレス情報を引数として受け取って上記文書ファイルに関するユーザのアクセス権限を認証する認証用プログラム部と、認証対象の文書ファイルのアドレス情報を上記認証用プログラム部に引数として渡すことを指示するリンク情報を保持するハイパーテキスト文書を記憶する文書記憶手段と、上記ブラウザに表示されている上記ハイパーテキスト文書中の上記リンク情報を利用して上記認証用プログラム部に上記認証対象の文書ファイルのアドレス情報を引数として送る手段と、上記認証対象の文書ファイルについて上記認証用プログラム部による認証が成功したときに、上記認証対象のファイルを上記ブラウザに供給する手段とを設けるようにしている。

【0007】この構成においては、所望の文書をアクセスする際には、認証用プログラム部のチェックを介在させるようにでき、ハイパーテキスト環境においても確実かつ容易にセキュリティを確保することができる。

【0008】また、この発明によれば、上述の目的を達成するために、文書表示装置に、ブラウザと、文書ファイルへのアドレス情報を引数として受け取って上記文書ファイルに関するユーザのアクセス権限を認証する認証用プログラム部と、認証対象の文書ファイルのアドレス情報を上記認証用プログラム部に引数として渡すことを指示するリンク情報を保持するハイパーテキスト文書を記憶する文書記憶手段と、上記ブラウザに表示されている上記ハイパーテキスト文書中の上記リンク情報を利用して上記認証用プログラム部に上記認証対象の文書ファイルのアドレス情報を引数として送る手段と、上記認証対象の文書ファイルについて上記認証用プログラム部による認証が成功したときに、上記認証対象のファイルを上記ブラウザに供給する手段と、上記認証対象の文書ファイルがハイパーテキスト文書の場合には、上記文書ファイルを上記ブラウザに送る前に、上記文書ファイルに含まれる他の文書ファイルへのリンク情報を、上記他の文書ファイルのアドレス情報を上記認証用プログラム部に引数として渡すことを指示するリンク情報に書き換える手段とを設けるようにしている。

【0009】この構成においても、所望の文書をアクセスする際には、認証用プログラム部のチェックを介在させるようにでき、ハイパーテキスト環境においても確実

かつ容易にセキュリティを確保することができる。しかも、リンク情報を用いて取出すハイパーテキスト文書中のリンク情報を自動的に書き換えるようにしているため、1のハイパーテキスト文書でリンク情報の書き換えを行っておけば、関連するリンク先の文書についてはなんら手作業で書き換えを行う必要がない。

【0010】この構成においては、たとえば上記ハイパーテキスト文書中の他の文書のアドレスは相対パスで記述される。

【0011】また、上記認証用プログラムはユーザがアクセスしようとしている文書が提供されるアプリケーションに関する情報を利用して上記ユーザのアクセス権限を認証するようにしてもよい。

【0012】また、上記認証用プログラム部による認証が失敗したときに上記ブラウザにエラーメッセージのコンテンツを供給するようにしてもよい。

【0013】また、この発明によれば、上述の目的を達成するために、ハイパーテキスト文書を利用したアプリケーション・サービスにおいてユーザのアクセス権限を認証するアクセス権限認証装置に、文書ファイルへのアドレス情報を引数として受け取って上記文書ファイルに関するユーザのアクセス権限を認証する認証用プログラム部と、ブラウザに表示されている上記ハイパーテキスト文書中のリンク情報を利用して上記認証用プログラム部に上記認証対象の文書ファイルのアドレス情報を引数として送る手段とを設けている。

【0014】この構成においても、所望の文書をアクセスする際には、認証用プログラム部のチェックを介在させるようにでき、ハイパーテキスト環境においても確実かつ容易にセキュリティを確保することができる。

【0015】また、この発明によれば、上述の目的を達成するために、アクセス権限認証装置において、リクエストに含まれるURLにより、認証を行うプログラムを指定するとともに、上記プログラムの引数として認証対象のファイルのアドレス情報を指定し、上記認証を行うプログラムにより上記認証対象のファイルについてユーザのアクセス権限を認証するようにしている。

【0016】この構成においても、所望の文書をアクセスする際には、認証用プログラム部のチェックを介在させるようにでき、ハイパーテキスト環境においても確実かつ容易にセキュリティを確保することができる。

【0017】また、この発明によれば、上述の目的を達成するために、文書を記憶し認証用プログラム部の認証が成功したときに文書を供給する文書サーバに、認証対象の文書ファイルのアドレス情報を上記認証用プログラム部に引数として渡すことを指示するリンク情報を保持するハイパーテキスト文書を記憶する文書記憶手段を設けている。

【0018】この構成においても、所望の文書をアクセスする際には、認証用プログラム部のチェックを介在さ

【0025】URL置換・出力処理部17は、ウェブページ中の通常のURL（ユニフォームリソースロケータ）を、データベース情報チェック処理部16によるチェックを指示するURL（データベース情報チェック処

【ステップS11】：プログラム起動引数から所定の情報を取得する。上の例では、アプリケーションID (AppID)、アプリケーションのバージョン (Ver)、現在表示されているウェブページの絶対パス (Doc)、

リンク先の相対パス (Next) 等を入力する。

【ステップ S 12】：初期情報、各種パラメータを設定する。

【ステップ S 13】：データベース 13 に情報照会を行ってユーザのアクセス権限等をチェックする。この処理は図 3 を用いて詳述する。

【ステップ S 14】：ステップ S 13 でチェック結果がアクセスを許可するものであれば、アクセス対象 (リンク先) のページを取出して出力する。取出したページが HTML ファイル (ウェブページ) の場合には、このページに含まれる URL を書き換える。この処理は図 4 を用いて詳述する。

【ステップ S 15】：書き換えたウェブページや画像 (画像にはとくに処理を行わない) 等、要求された文書を表示用ブラウザ 10 に送り処理を終了する。

【0032】図 3 は、チェック処理を示しており、ユーザのアクセス権限やアプリケーションの有効・無効を判断する。このチェック処理は以下のとおりである。

【0033】【ステップ S 16】：チェック処理のルーチンが開始される。

【ステップ S 17】：ユーザに対する認証をチェックする。このチェックはデータベース 13 のアプリケーション情報を参照して行う。

【ステップ S 18】：ユーザのアクセスが認められた場合にはステップ S 19 へ進み、認められなかった場合にはステップ S 23 へ進む。

【ステップ S 19】：アプリケーション情報の有効無効を判断する。有効であればステップ S 20 へ進み、無効であればステップ S 23 へ進む。

【ステップ S 21】：表示対象ドキュメントのディレクトリ位置が適切かどうかを判断する。例えば、HTML ファイルや画像ファイルは所定の基準ディレクトリより下かどうかを判断する。下であれば、そのままアクセスを許可しステップ S 21 へ進み、そうでなければアクセスを許可せずステップ S 23 に進む。

【ステップ S 21】：データベースから取得した情報を次処理のために保持する。

【ステップ S 22】：メインルーチンへ戻る。

【ステップ S 23】：エラーの内容に応じて対応するエラーメッセージを選択する。

【ステップ S 24】：エラーメッセージを画面出力する。

【ステップ S 25】：エラー処理を終了する。

【0034】つぎに URL 置換・出力処理部 17 の動作について図 4 を参照して説明する。URL 置換・出力処理部 17 の処理は以下のとおり行われる。

【0035】【ステップ S 26】：URL 置換・出力ルーチンが開始される。

【ステップ S 27】：表示対象文書が HTML ファイルかその他のファイルか判別する。HTML ファイルの場合のみ URL 置換が必要である。HTML ファイルの場合

ステップ S 28 へ進み、その他のファイルの場合ステップ S 34 へ進む。

【ステップ S 28】：置換処理用に初期値を設定する。

【ステップ S 29】：ステップ S 29～ステップ S 33 の処理は HTML 文 1 行ごとに繰返される。まず、ステップ S 29 において、HTML 文を 1 行読み込む。

【ステップ S 30】：対象 HTML ファイルにおいてファイル終了 (EOF) が検出されたかどうか判別する。ファイル終了であれば、ステップ S 38 へ進み処理を終了し、ファイル終了でなければ、ステップ S 31 へ進む。

【ステップ S 31】：URL 記述箇所があるかどうかを判別する。なければステップ S 34 へ進み、あればステップ S 32 へ進む。なお、この実施例では、アンカータグは 1 行に 1 つとなるように記述するものとする。1 行に複数箇所のアンカータグを許容する場合には、アンカータグごとに処理ループを構成する。

【ステップ S 32】：URL が置換対象となる URL であるかどうかを判断する。相対パスで指定されたセキュリティの URL ならば、ステップ S 33 へ進み置換処理を行なう。セキュリティ対象外 URL もしくはフルパス指定された URL は、置換対象外であるため、ステップ S 34 へ進む。

【ステップ S 33】：URL をチェックプログラム経由の URL に置き換える。

【ステップ S 34】：読み込んだ 1 行分の HTML 文を標準出力する。この後、ステップ S 29 へ戻る。

【ステップ S 35】：表示対象文書が HTML ファイルでない場合の処理であり、ファイル拡張子に応じて MIME タイプを設定する。

【ステップ S 36】：ファイルから 1 行読み込む。

【ステップ S 37】：ファイル終了 (EOF) かどうかを判断し、ファイル終了であればステップ S 39 へ進み処理を終了する。ファイル終了でなければ、ステップ S 38 へ進む。

【ステップ S 38】：読み込んだ 1 行をそのまま標準出力し、ステップ S 35 へ戻る。

【ステップ S 39】：処理を終了しメインルーチンへ戻る。

【0036】最後に、全体的な動作について概観しておく。図 5 はウェブサーバ 15 の文書記憶部 12 に記憶されている文書 (ページ) を示している。この図の例では、サービスのホームページ (index.htm) 30 において他のページ (sample1.htm、sample2.htm) 31、32 がリンクされ、さらにページ 311、321 等がリンクされている。この例において、ホームページ 30 のページ 31、32 に対する URL を、チェック・URL 置換プログラム経由の URL とする。このようにするとページ 31、32、31

1、312についてセキュリティをかけることができる。例えば、ユーザがホームページ30においてページ31へのチェック・URL置換プログラム経由のURLをクリックするとページ31に対するユーザのアクセス権限が認証される。そして認証が成功すると、ページ31がブラウザ10に表示される。この際、ページ31に含まれるページ311等へのURLはチェック・URL置換プログラム経由のURLに置き換えられる。したがって、表示されているページ31においてページ311のURLをクリックするとページ311に対する認証が行われる。同様にページ32、ページ321等についても認証が行われる。このように、チェック・URLプログラム経由のURLの記述を1つ行えば、そこから直接又は間接にリンクされているページについてもセキュリティが確保される。

【0037】以上説明したように、この実施例においては、アンカータグを用いてリンク先のターゲットファイルを指定する際に、チェックプログラム経由となるようにしているため、HTMLのリンク情報により分散して配置された文書でも確実かつ容易にユーザのアクセス権限の認証を行うことができる。またアドレスごとにチェック機能を付加する必要もない。さらに、この実施例では、ターゲットファイル中にURLが含まれている場合にはこのURLをチェックプログラム経由となるように自動的に書き換えているので、ファイル記述をわずかに修正するだけで、多くの文書についてユーザのアクセス権限の認証を行うことができる。

【0038】なお、この発明は上述の実施例に限定されるものではなく、その趣旨を逸脱しない範囲で種々変更が可能である。例えば、ハイパーテキストとしてはHTMLに限らず、XML（エクステンシブルマークアップラングエッジ）やコンパクトHTML等でもよい。また、プログラムはCGIでなく、SSI等で構成してもよい。

【0039】また、URLの書き換えを行わずに、単にチェックのみを行うようにしてもよい。この場合、セキ

ュリティが必要な文書へのリンクはチェックプログラム経由のURLにする。また、文書ファイルを組み込んだ後、URL置換プログラムで一度にURLを置換するようにしてもよい。

【0040】

【発明の効果】以上説明したように、この発明によれば、HTMLファイル等ハイパーテキスト文書に含まれるリンク情報をチェック手段経由の形式として保持するようにしたので、1つのチェック手段で簡単に多くの文書のアクセス権限をチェックすることができる。また、チェックのみでなくURL置換も行うようにすれば、簡単に多くのファイルをセキュリティ対象下に置くことができる。

【図面の簡単な説明】

【図1】 この発明の実施例を全体として示すブロック図である。

【図2】 上述実施例の動作を全体として示すフローチャートである。

【図3】 図2のステップ13の動作を詳細に示すフローチャートである。

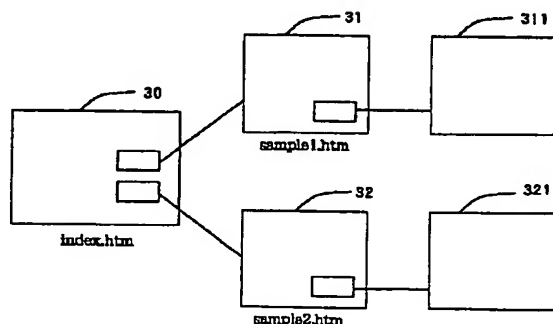
【図4】 図2のステップ14の動作を詳細に示すフローチャートである。

【図5】 上述実施例の全体的な動作を説明する図である。

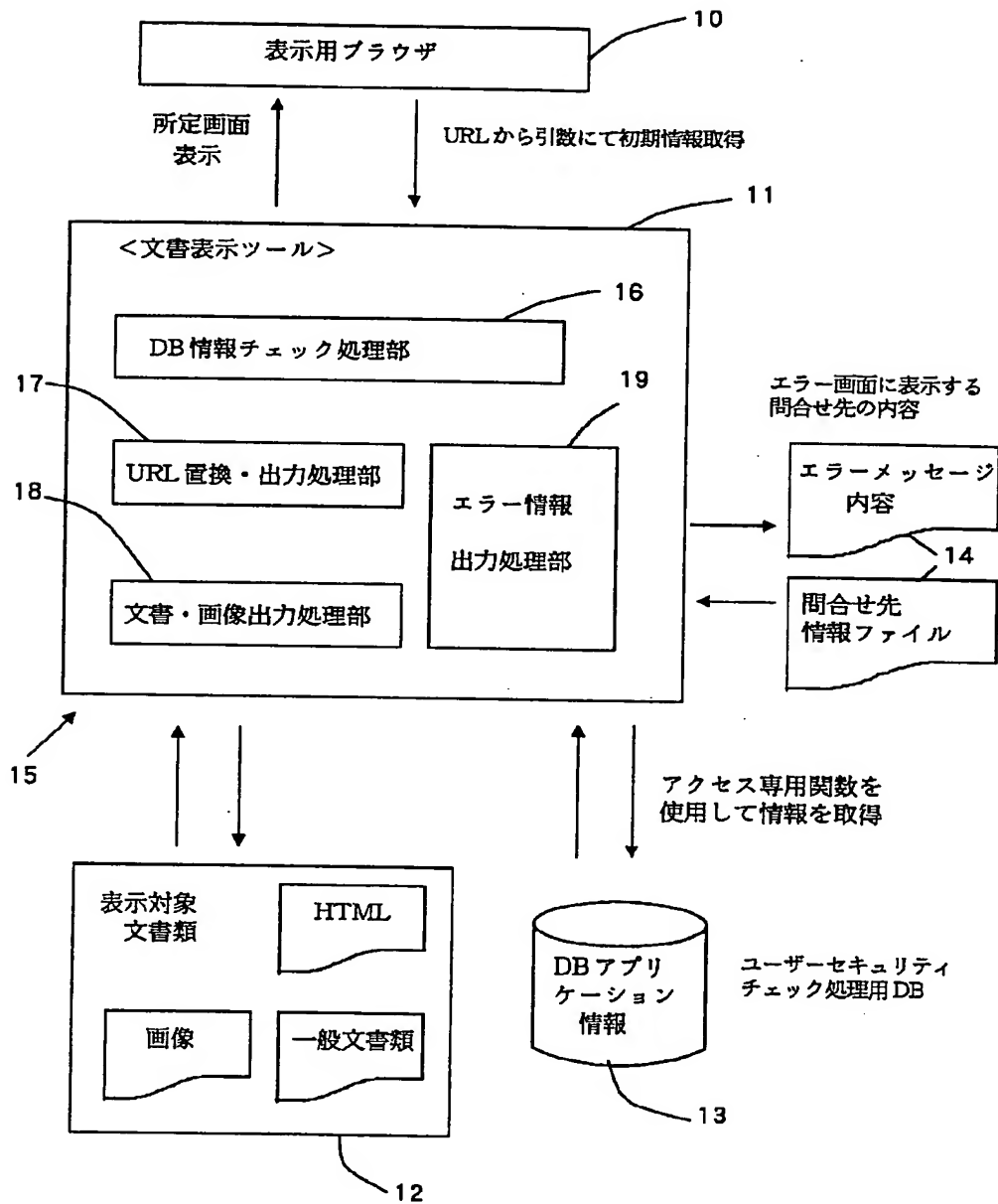
【符号の説明】

- 10 表示用ブラウザ
- 11 文書表示ツール
- 12 文書記憶部
- 13 データベース
- 14 エラーメッセージ記憶部
- 15 ウェブサーバ
- 16 データベース情報チェック処理部
- 17 URL置換・出力処理部
- 18 文書・画像出力処理部
- 19 エラー情報出力処理部

【図5】



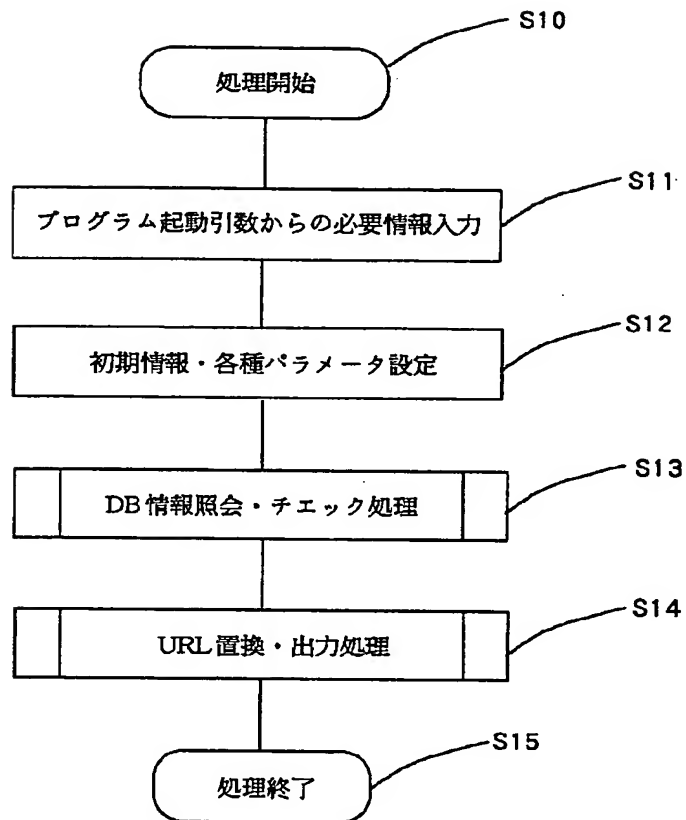
【図1】



*「一般文書」とは、ワープロソフトや表計算ソフト
その他で作成された文書類を指す

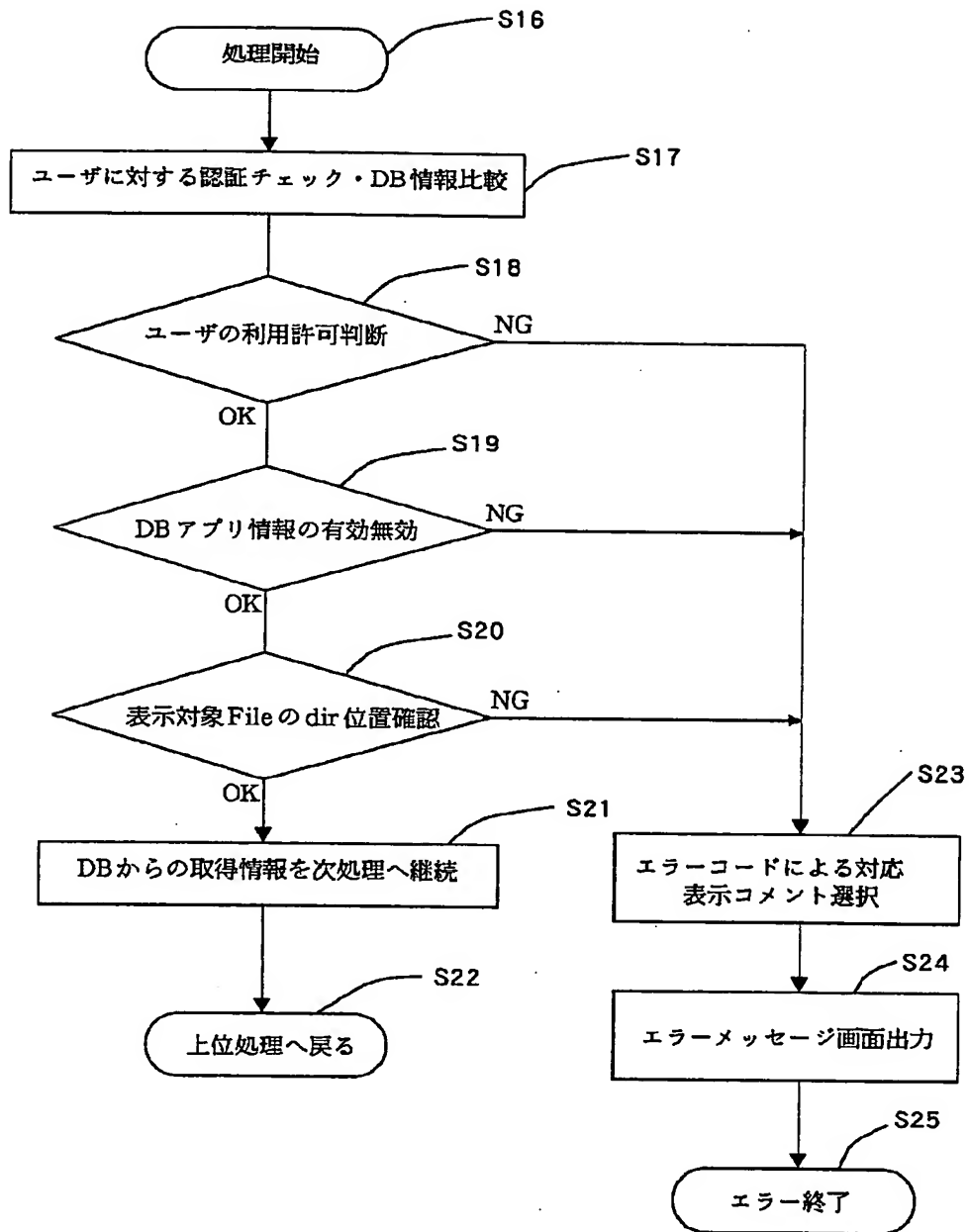
【図2】

全体処理フロー



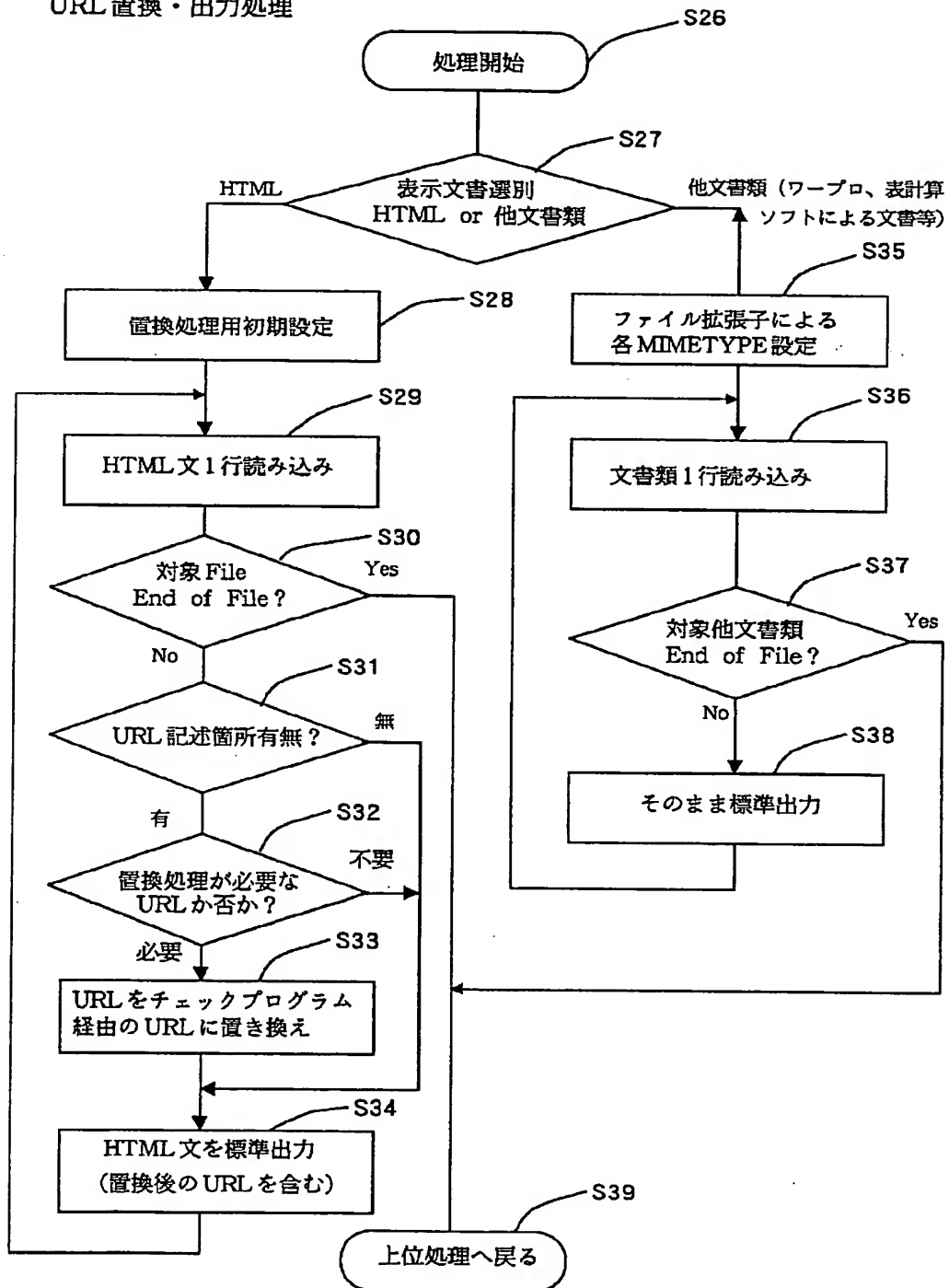
【図3】

DB情報照会・チェック処理



【図4】

URL 置換・出力処理



フロントページの続き

(51) Int. Cl.⁷

識別記号

F I

テ-マ-ト (参考)

G 0 6 F 15/40

3 7 0 A

(72) 発明者 堀 究

神奈川県海老名市本郷2274番地 富士ゼロ
ックス株式会社海老名事業所内F タ-ム (参考) 5B075 KK02 KK44 KK63 ND03 NK44
PQ42
5B082 EA00 EA01 EA11
5B085 AE06 AE23 BE07 BG07